

Fig. 1

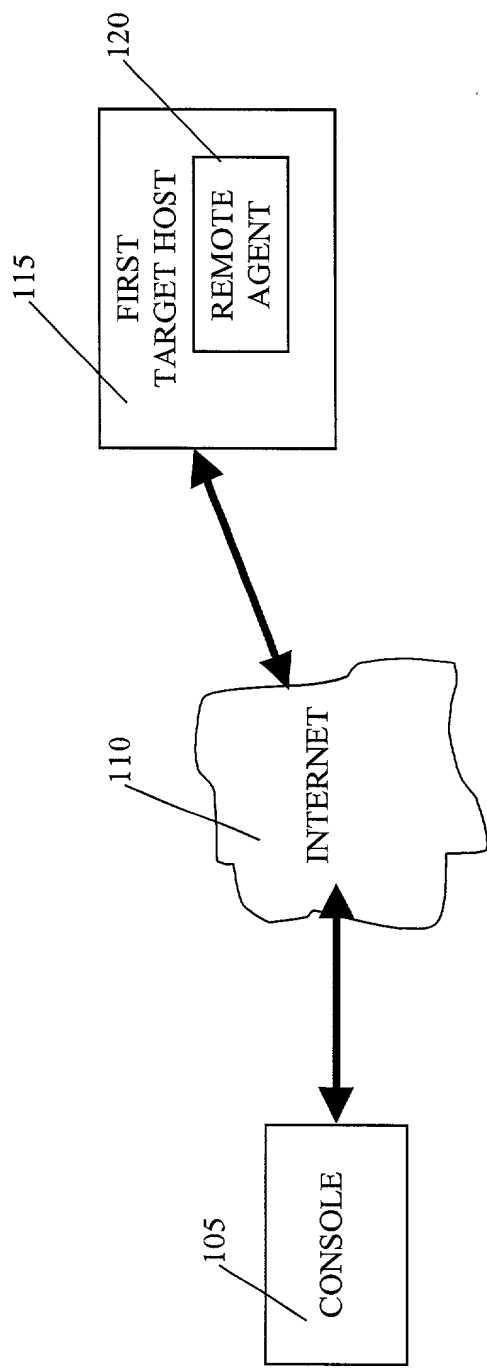


Fig. 2

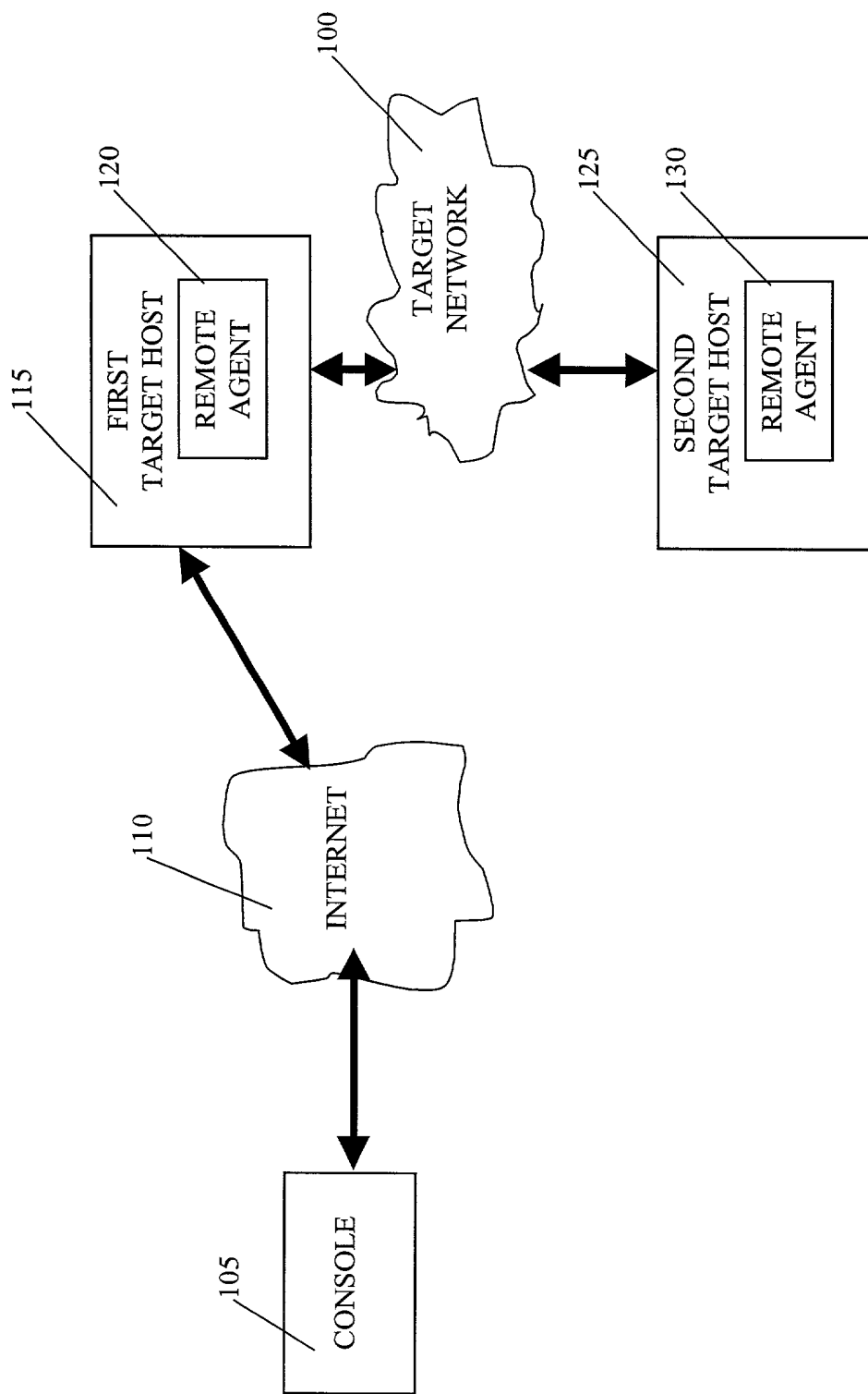


Fig. 3

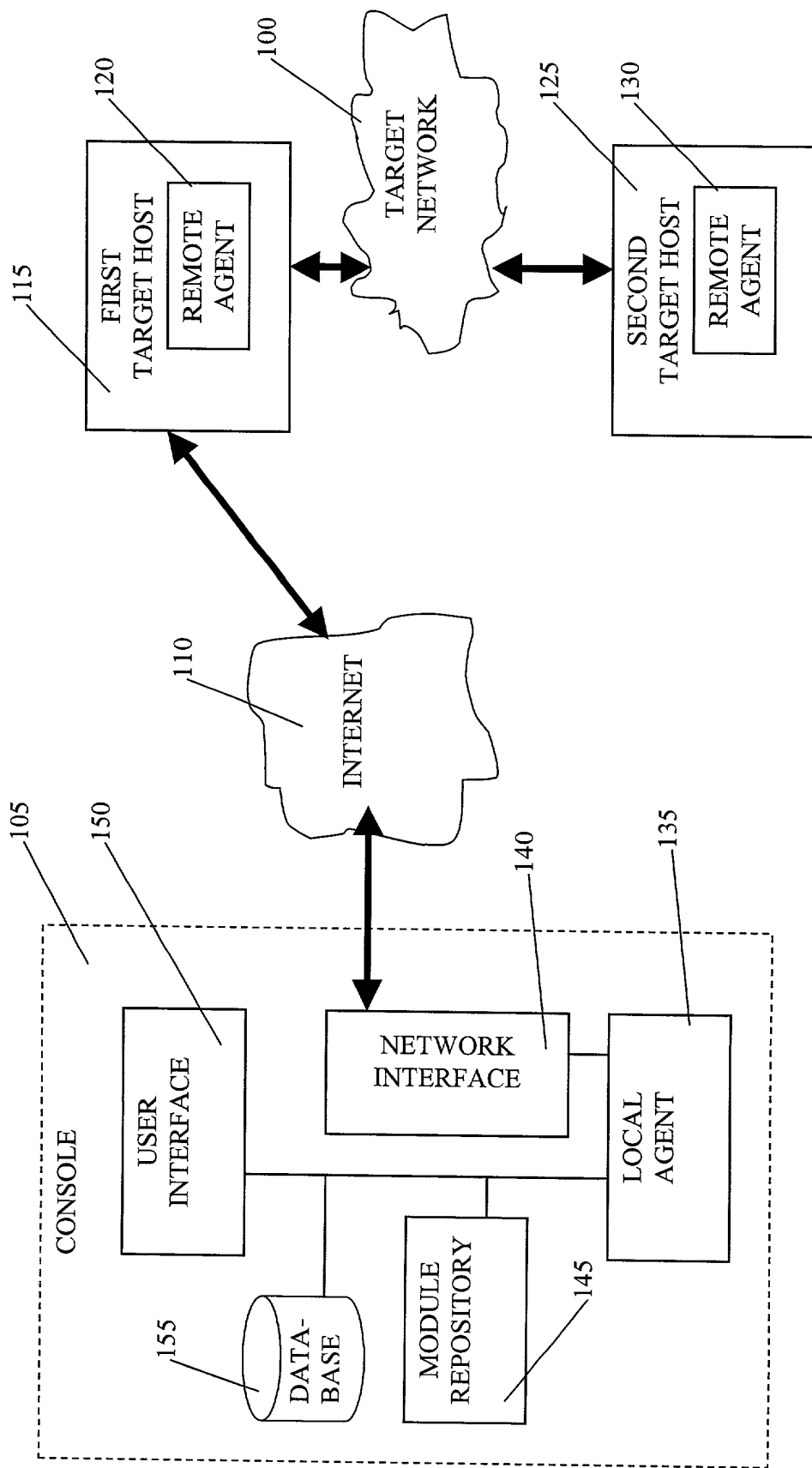


Fig. 4

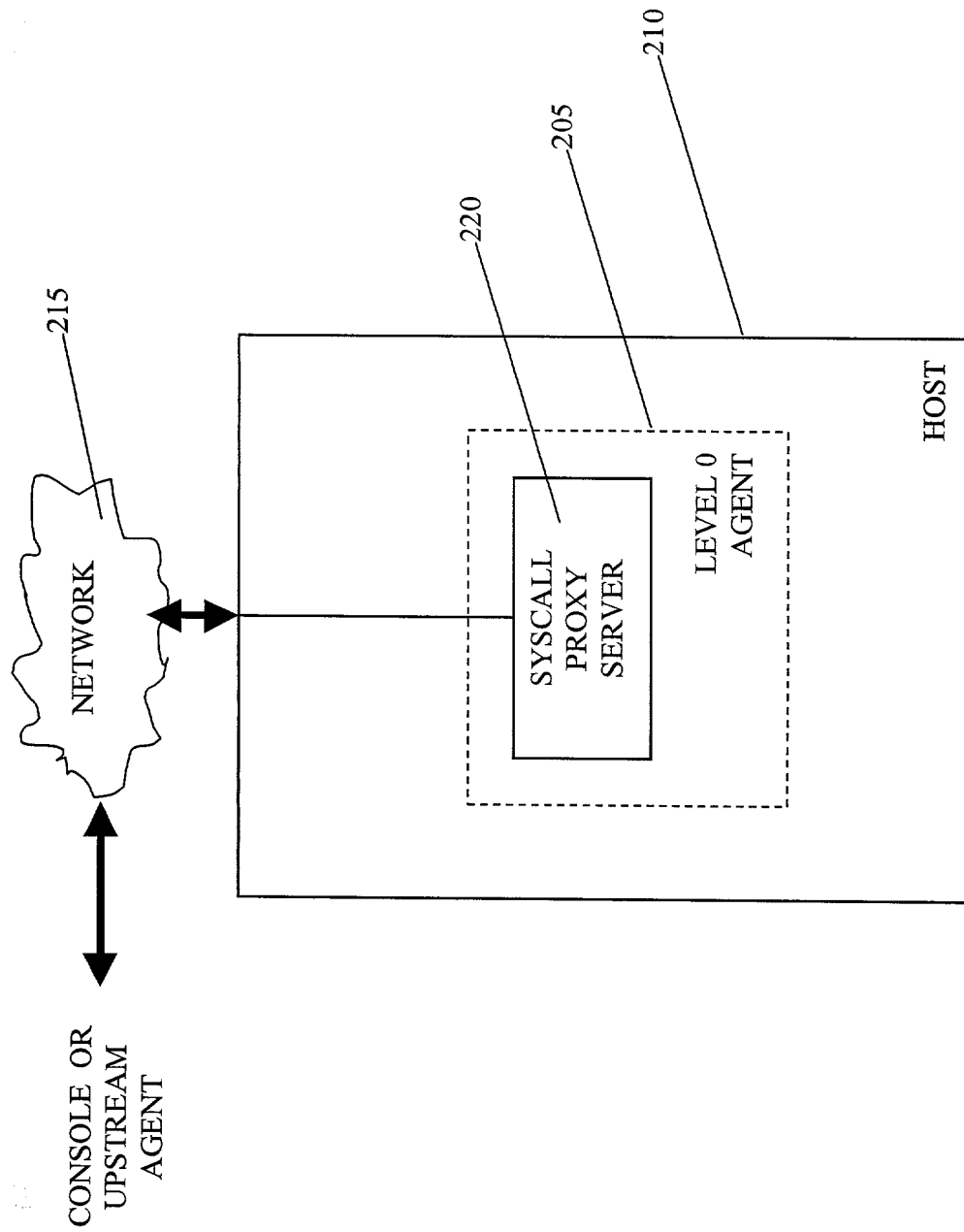


Fig. 5

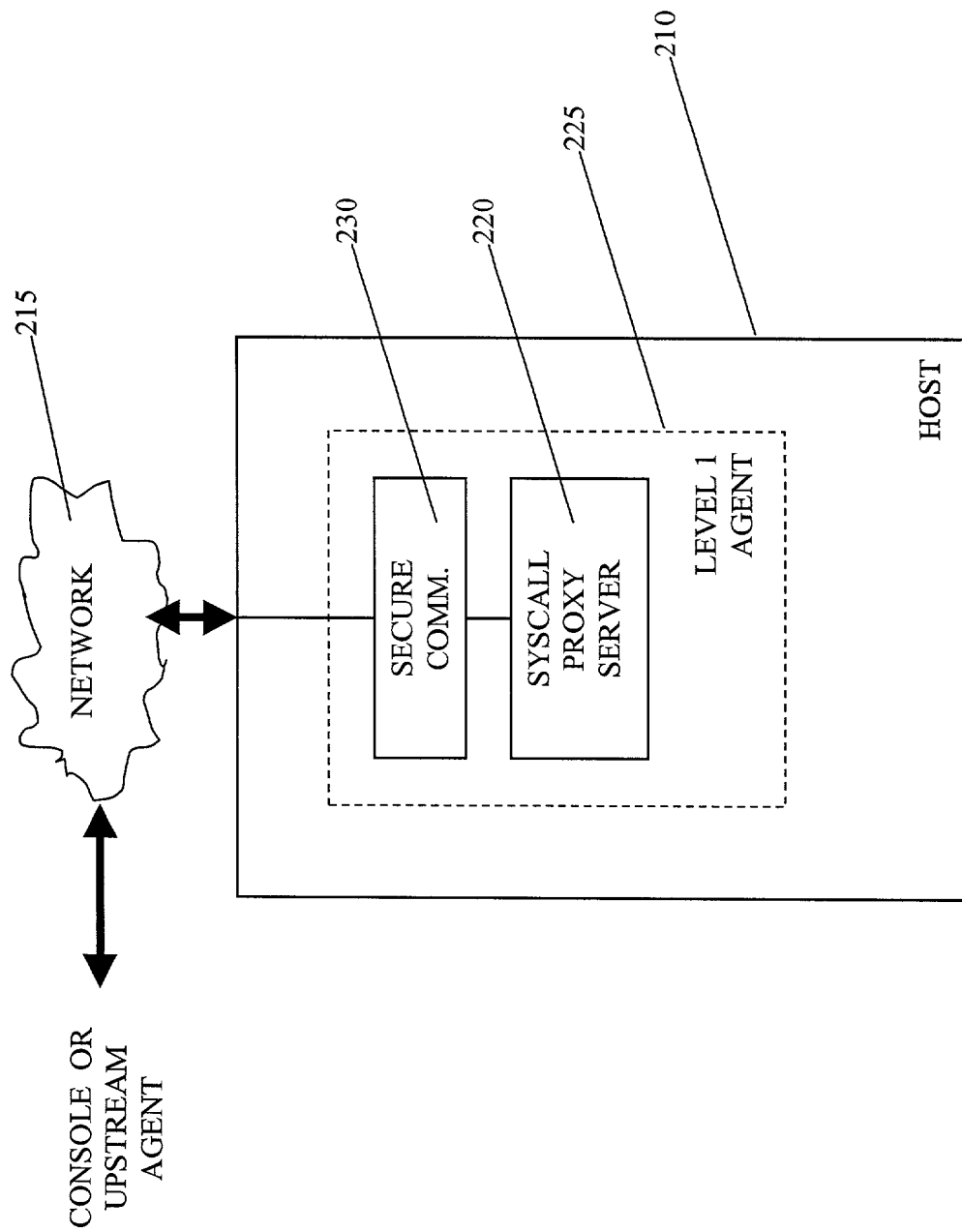


Fig. 6

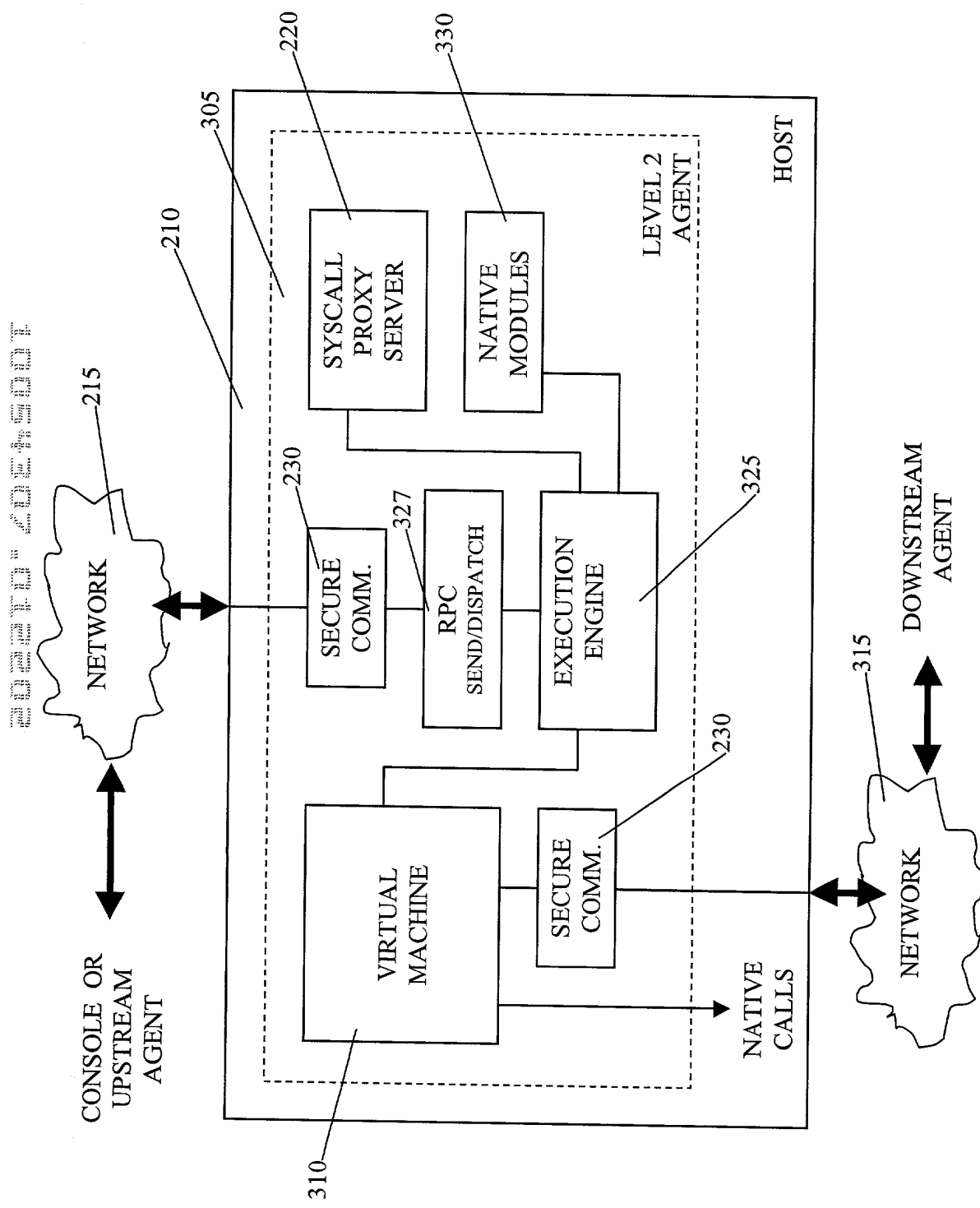


Fig. 7

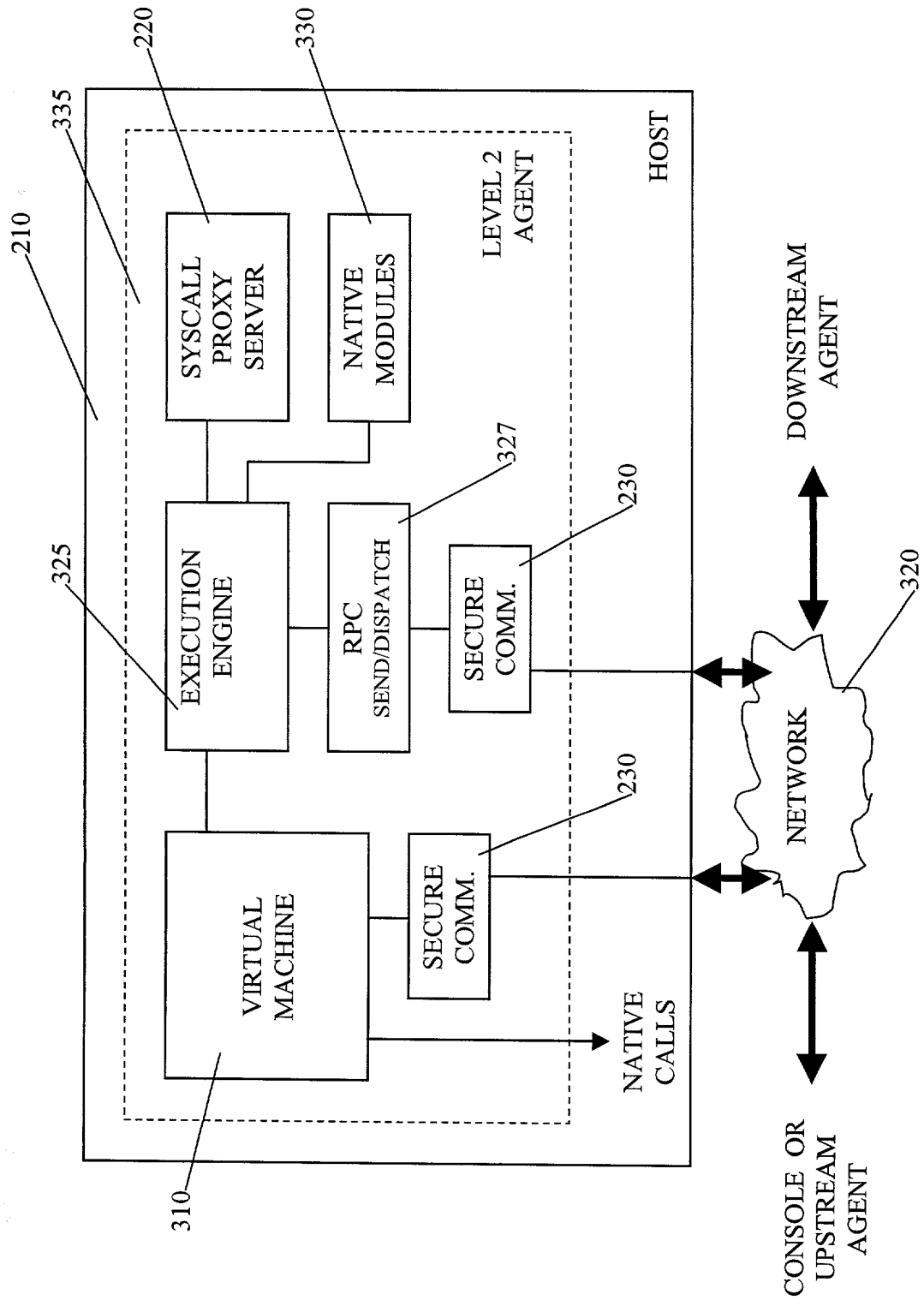


Fig. 8



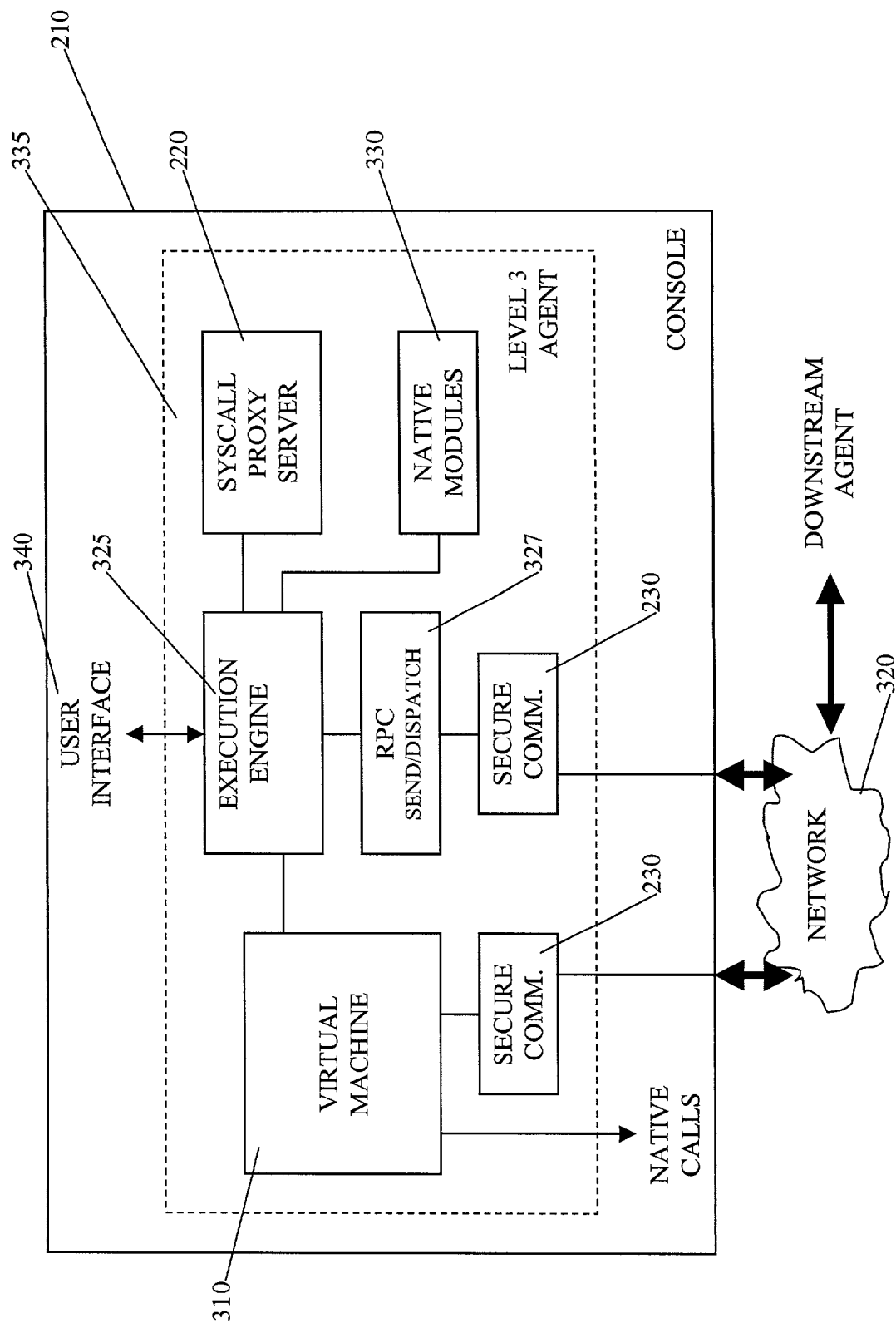


Fig. 9

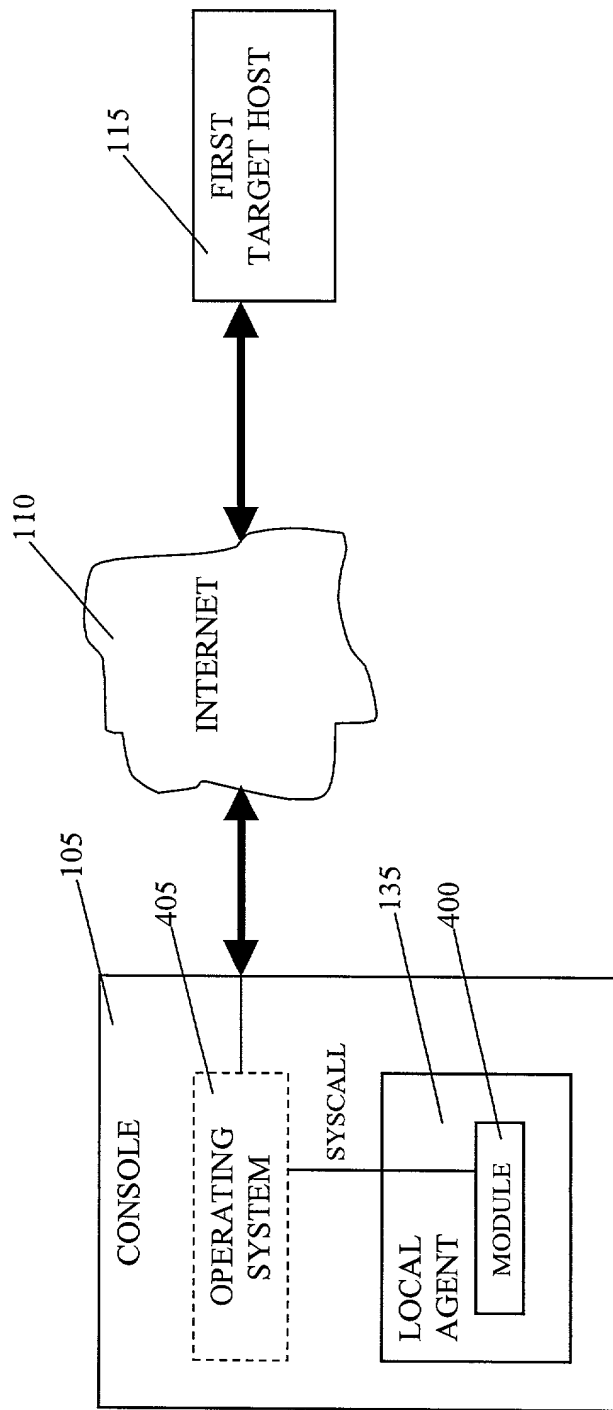


Fig. 10

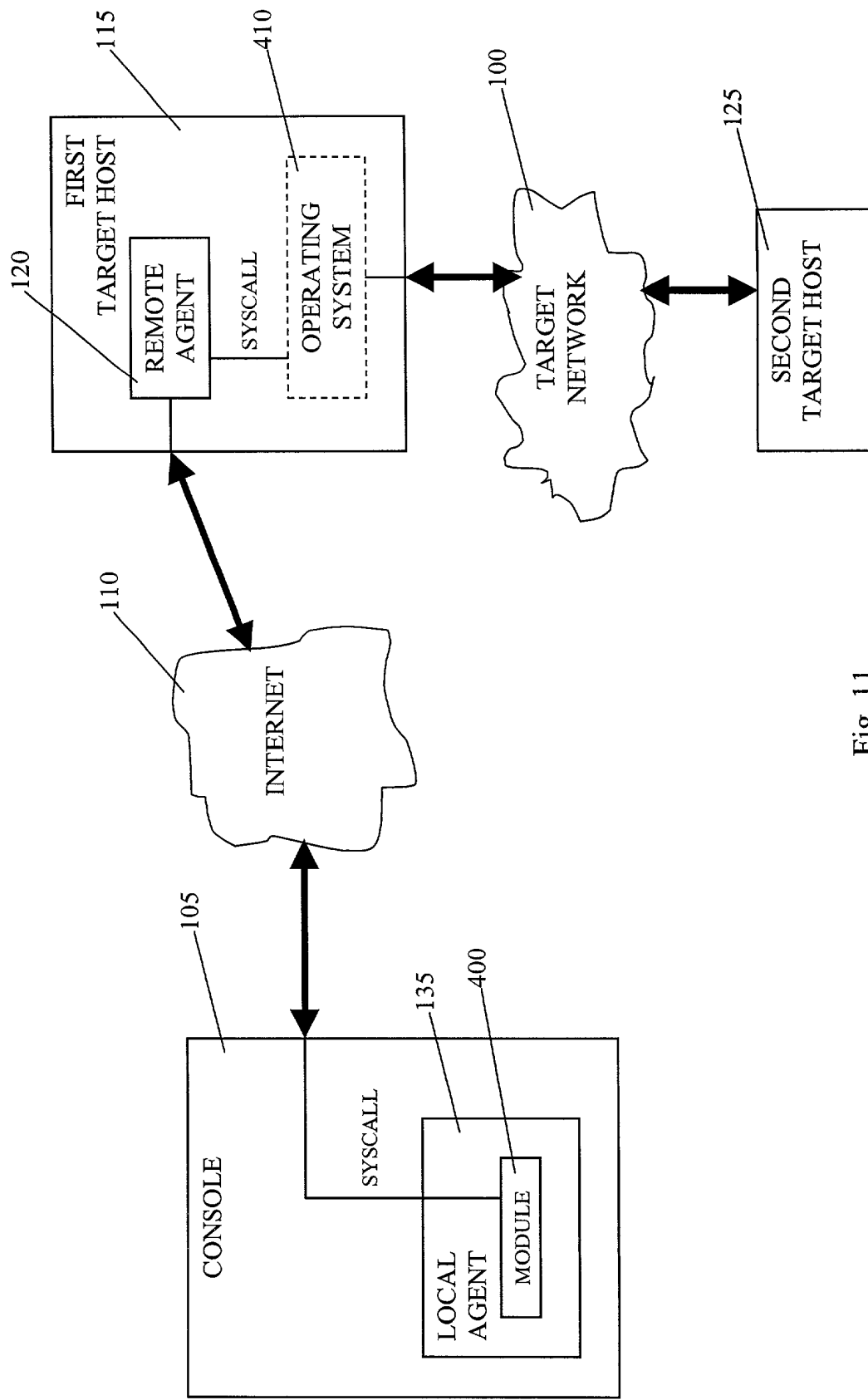


Fig. 11

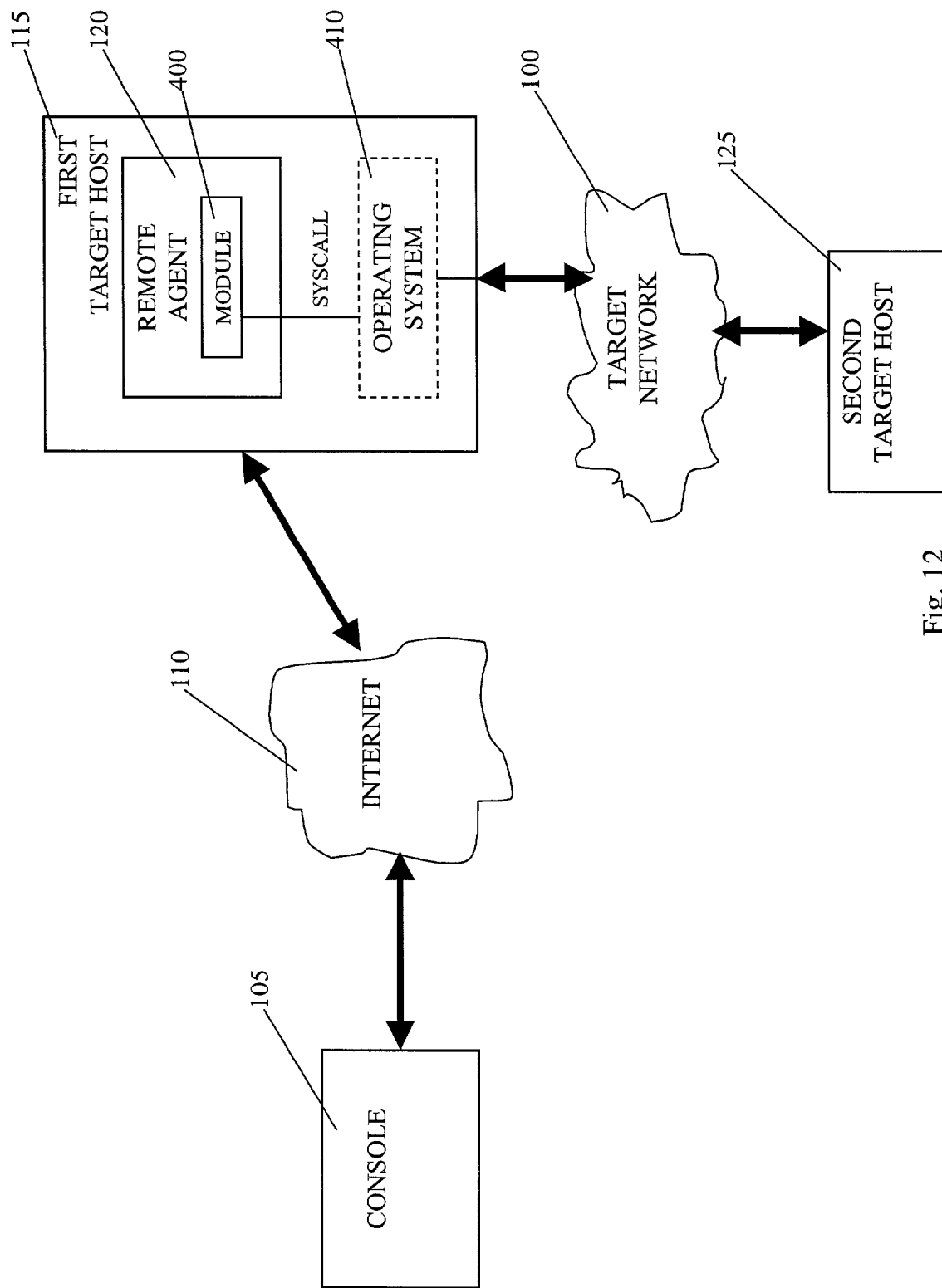


Fig. 12

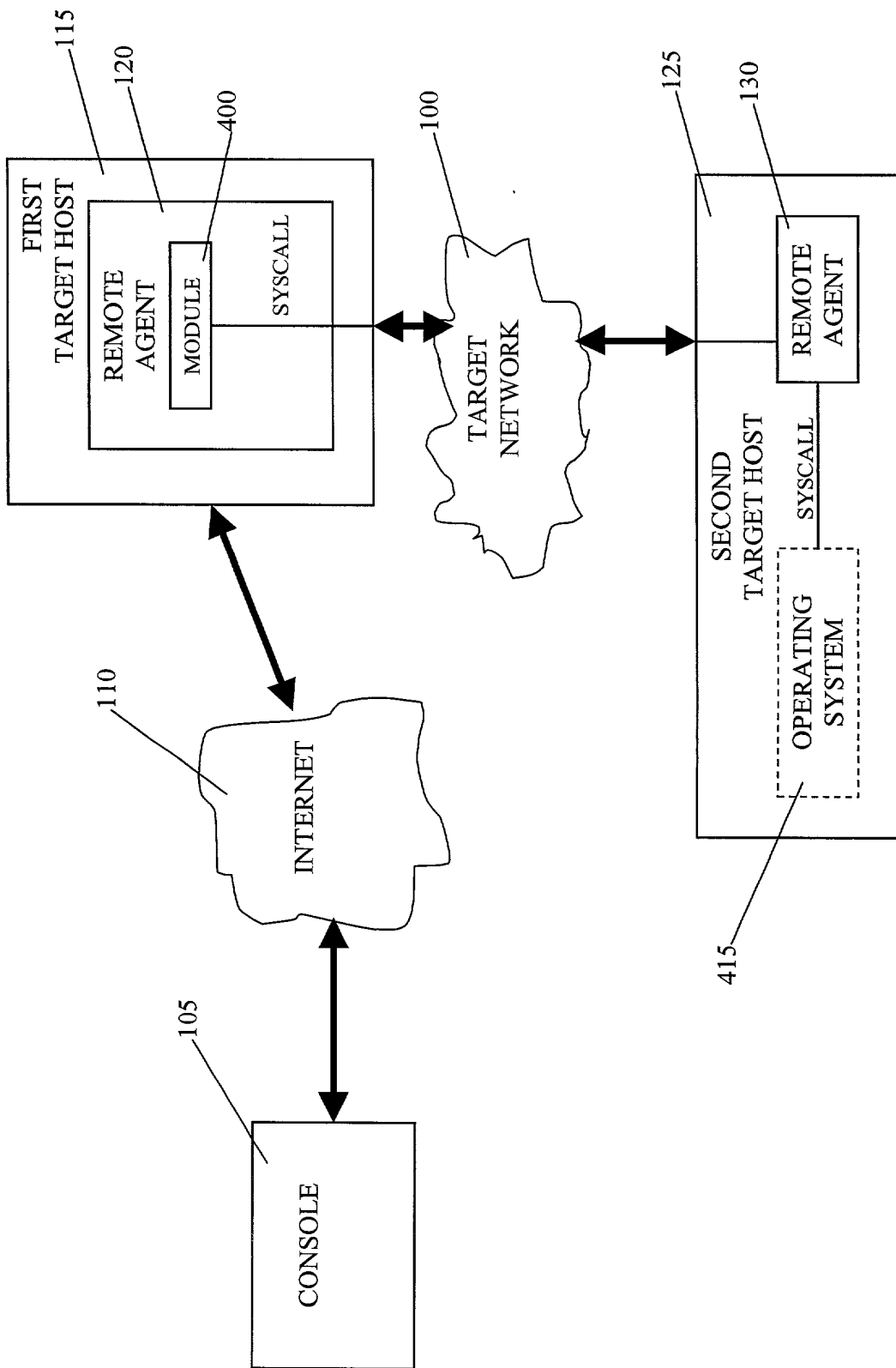


Fig. 13



20220707 10:44:00

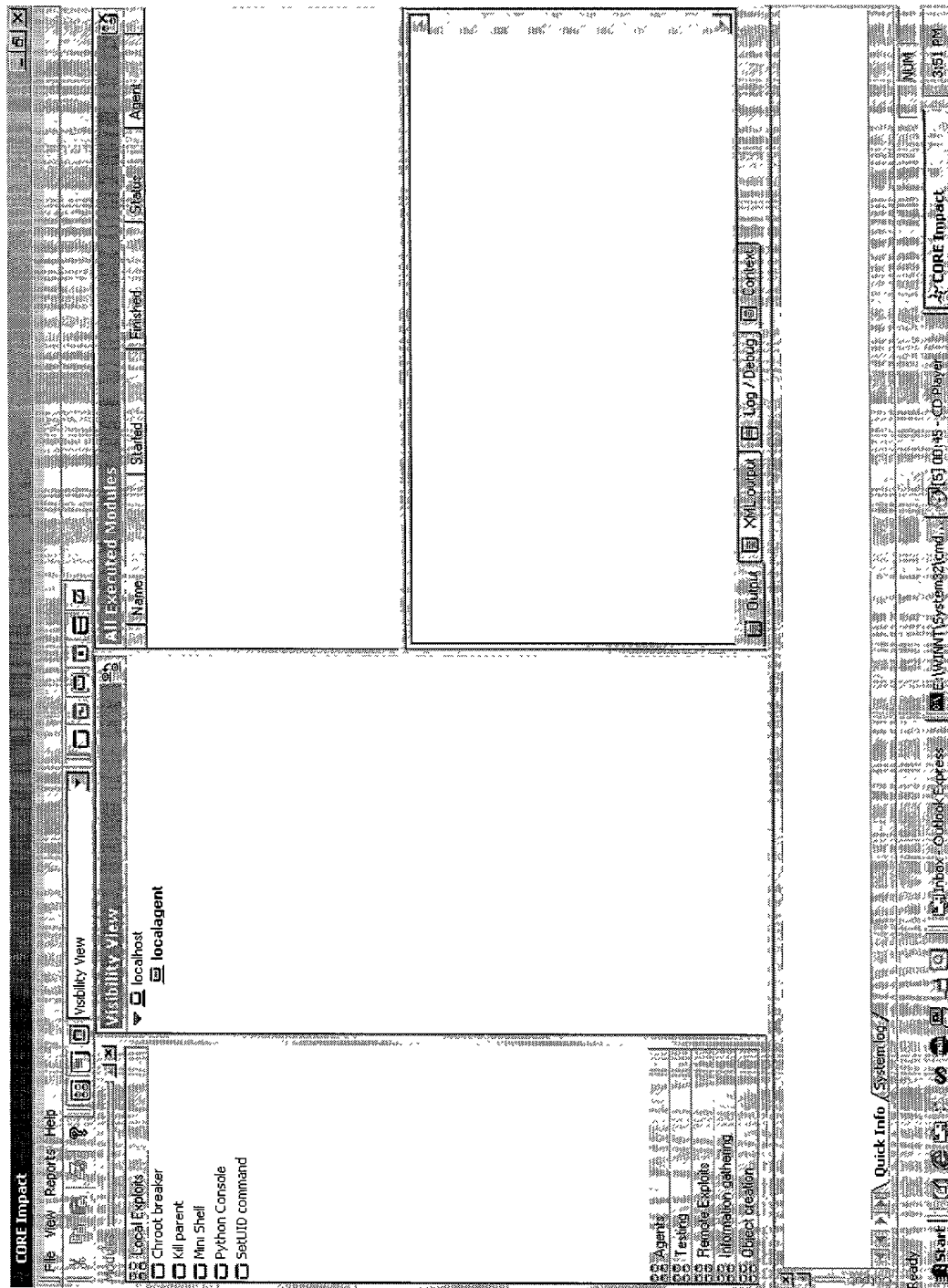


Fig. 15

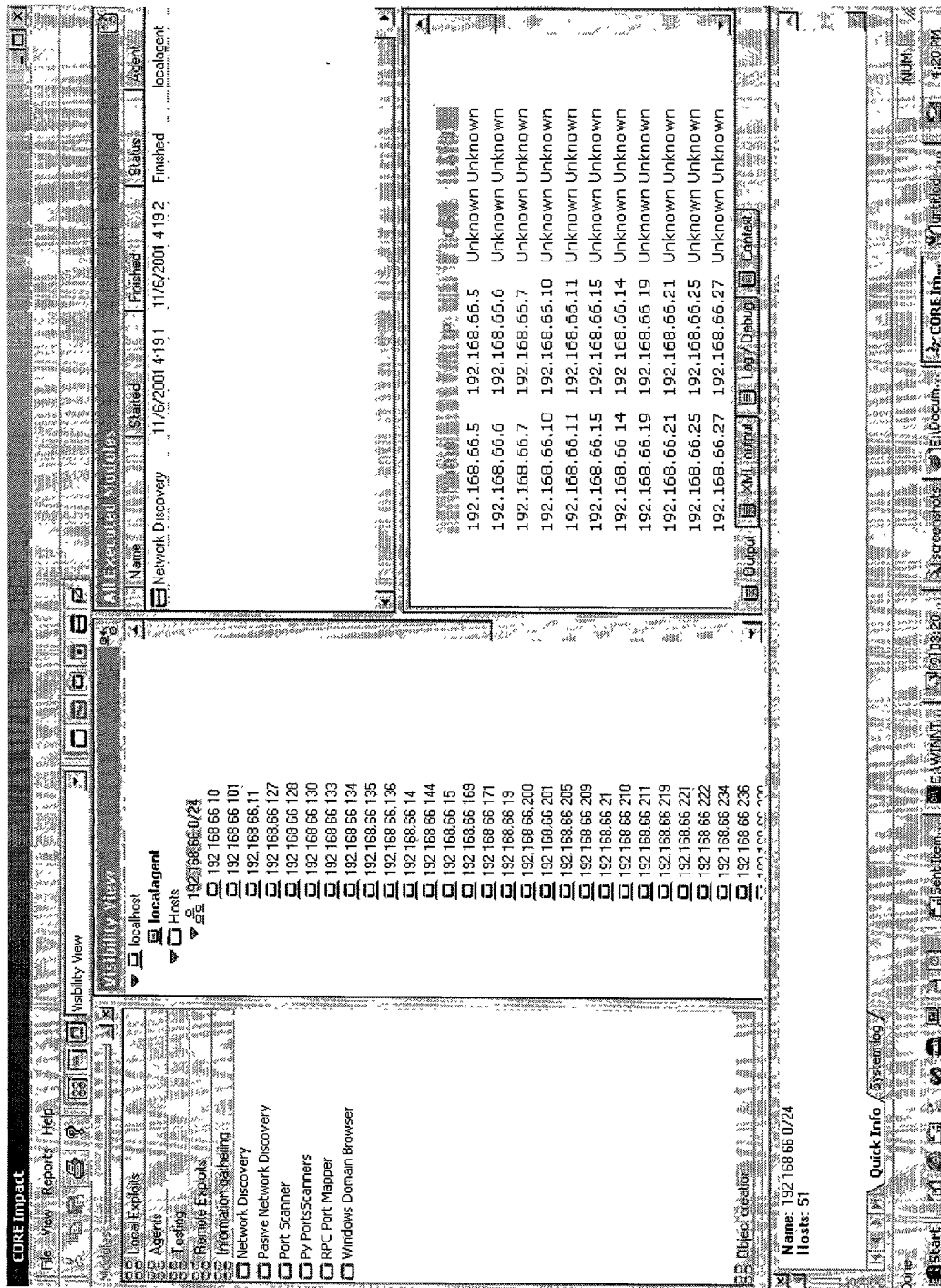


Fig. 16



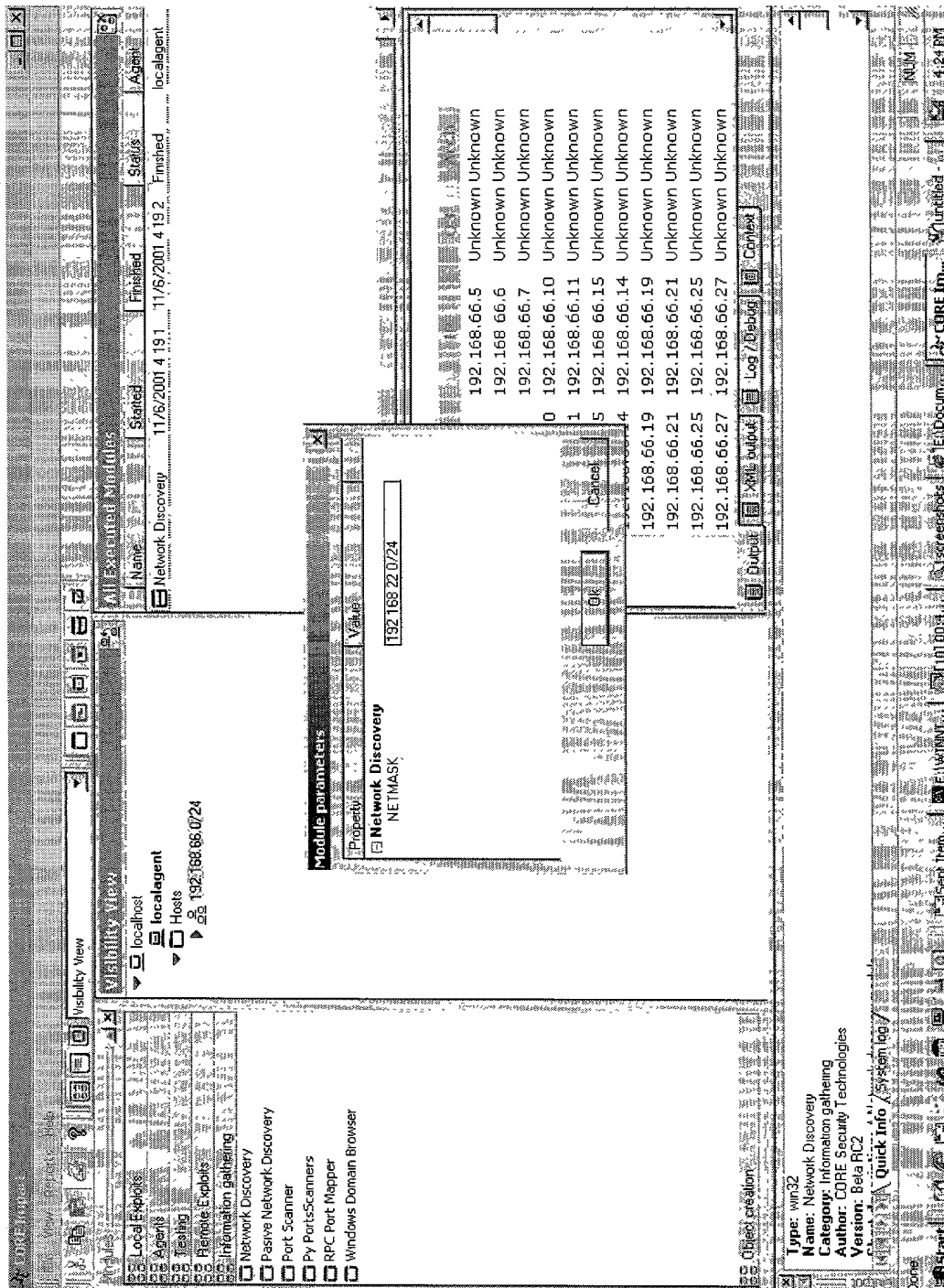


Fig. 17

2007-06-16 00:00

CORE Impact

File View Reports Help

Visibility View

Local Exploits

Agents

Testing

Remote Exploits

Information gathering

Network Discovery

Passive Network Discovery

Port Scanner

Py PortsScanners

RPC Port Mapper

Windows Domain Browser

Visibility View

localhost

localagent

Hosts

192.168.65.0/24

192.168.22.0/24

192.168.22.1

192.168.22.2

192.168.22.3

192.168.22.4

192.168.22.6

192.168.22.7

192.168.22.8

192.168.22.9

All Executed Modules

Name	Started	Finished	Status	Agent
Network Discovery	11/6/2001 4:19.1	11/6/2001 4:19.2	Finished	localagent
Network Discovery	11/6/2001 4:25.0	11/6/2001 4:25.0	Finished	localagent
RPC Port Mapper	11/6/2001 4:25.2	11/6/2001 4:25.2	Finished	localagent

Module "RPC Port Mapper" started execution on Tue Nov 06 16 25 23 2001

program	vers	proto	port
100000	4	tcp	111
100000	3	tcp	111
100000	2	tcp	111
100000	4	udp	111
100000	3	udp	111
100000	2	udp	111
100000	10	udp	32772
100011	1	udp	32773
100002	2	udp	32774
100002	3	udp	32774
100024	1	udp	32775
100024	1	tcp	32771
100133	1	udp	32775
100133	1	tcp	32771
100002	2	tcp	32772
100002	3	tcp	32772

Output

XML output

Log/Debug

Context

Name: 192.168.22.0/24

Hosts: 8

Done

Start

Quick Info / Systemlog

Core m...

Running on

4:25 PM

Fig. 18

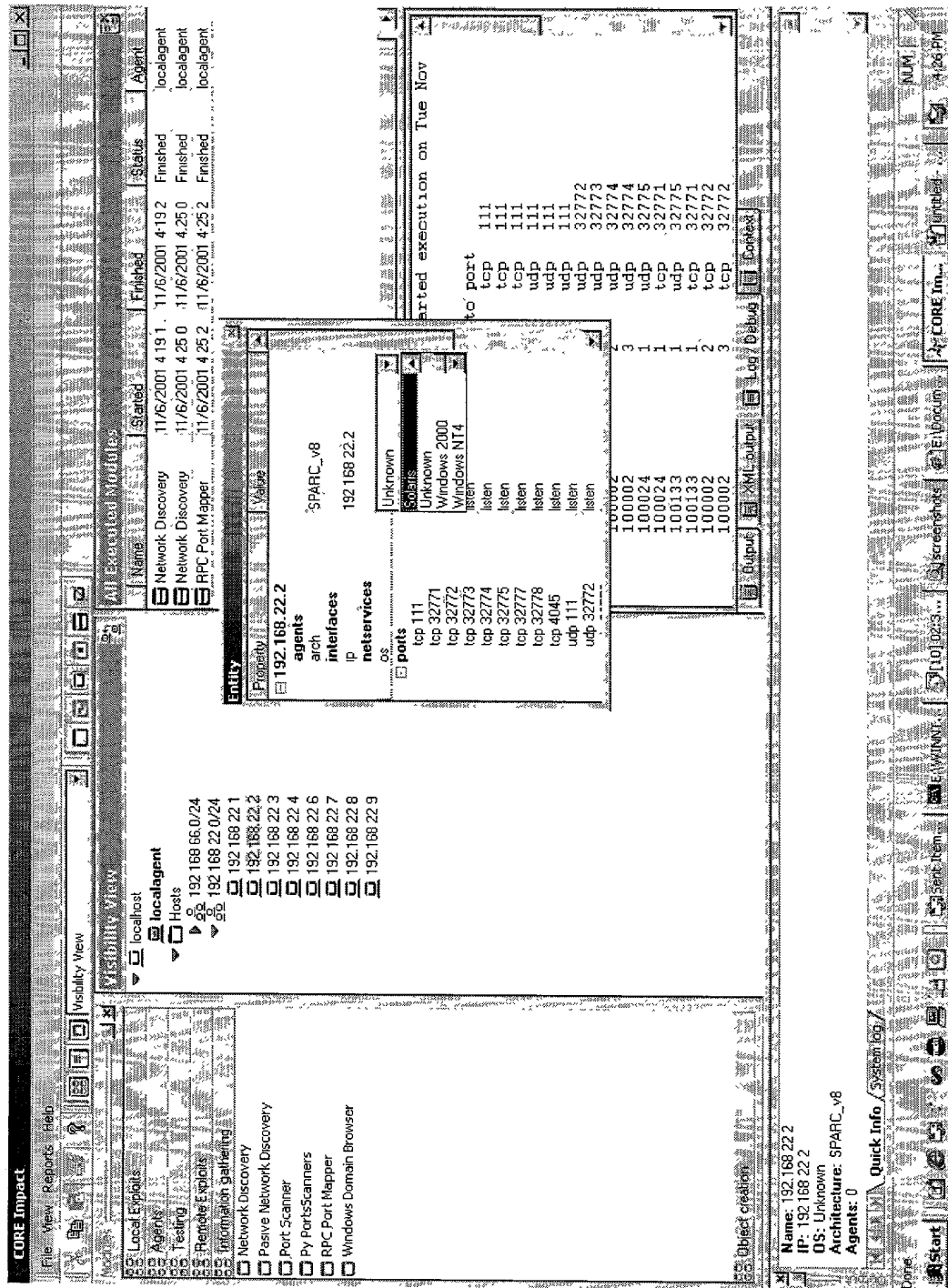


Fig. 19

**CORE Impact**

File View Reports Help Visibility View

**Local Exploits**

- Create Level 0 Service
- Create Level 1 Service
- Level 0 Agent
- Level 1 Agent

**Agents**

- localagent
- Hosts
- 192.168.22.4
- 192.168.22.0/24
- 192.168.22.1
- 192.168.22.2
- 192.168.22.3
- 192.168.22.4
- 192.168.22.6
- level0agentservice(0)
- level0(a)
- 192.168.22.7
- 192.168.22.8
- 192.168.22.9

**Testing**

- Remote Exploits
- Information gathering
- Object election

Property	Value
agents	Unknown
arch	Unknown
interfaces	192.168.22.4
ip	Unknown
netservices	Unknown
os	Unknown
ports	Unknown
windows domain	Unknown

**Quick Info / System Info**

Name: 192.168.22.4  
IP: 192.168.22.4  
OS: Unknown  
Architecture: Unknown  
Agents: 0

**Visibility View**

**localagent**

- Hosts
- 192.168.22.4
- 192.168.22.1
- 192.168.22.2
- 192.168.22.3
- 192.168.22.4
- 192.168.22.6
- level0agentservice(0)
- level0(a)
- 192.168.22.7
- 192.168.22.8
- 192.168.22.9

**All Executed Modules**

Name	Scheduled	Finished	Status	Agent
Network Discovery	11/6/2001 4:19:1	11/6/2001 4:19:2	Finished	localagent
Network Discovery	11/6/2001 4:25:0	11/6/2001 4:25:0	Finished	localagent
RPC Port Mapper	11/6/2001 4:25:2	11/6/2001 4:25:2	Finished	localagent
General exploit	11/6/2001 4:27:1	11/6/2001 4:27:1	Aborted	localagent
General exploit	11/6/2001 4:27:3	11/6/2001 4:27:3	Finished	localagent
Level 0 Agent	11/6/2001 4:27:4	11/6/2001 4:27:4	Finished	localagent

Module "Level 0 Agent" started execution on Tue Nov 06 16:27:40 2001

```
Creating Level0Agent using service level0agentservice(0) on host 192.168.22.6
Level 0 Agent' level0(a) created
Module finished execution after 1 secs
```

Detailed XML Output Debug Context

Fig. 20

2022-11-06 15:00

The screenshot displays the CORE Security Technology Python Console interface. The main window is divided into several panes:

- Left Pane (Modules):** Lists various modules including Local Exploits, Chroot breaker, Kill parent, Mini Shell, Python Console, SetUID command, Agents, Remote Exploits, Information gathering, and Object creation.
- Top Pane (All Executed Modules):** A table showing the execution status of various modules.
- Bottom Left Pane (Property):** Displays the current module's properties, including the author (level0(a)) and the module name (level0(a)).
- Bottom Right Pane (Terminal):** A terminal window showing the output of the Python Console, including the welcome message and the execution of the 'level0(a)' module.

Name	Status	Finished	Agent
Network Discovery	Finished	11/6/2001 4:19:1	localagent
RPC Port Mapper	Finished	11/6/2001 4:25:0	localagent
General exploit	Aborted	11/6/2001 4:25:2	localagent
Level 0 Agent	Finished	11/6/2001 4:27:1	localagent
Python Console	Finished	11/6/2001 4:27:3	level0(a)
Python Console	Running	11/6/2001 4:29:2	level0(a)

Module "Python Console" started execution on Tue Nov 06 16:29:22 2001

Entering Python Console using interpreter default

```
Welcome to Python Console. Using interpreter: default
Type 'exit' to exit
# import socket
# print socket.gethostname()
diavolo
# s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM, 0)
# s.bind(('0.0.0.0', 0))
# print s
# socket._socketobject instance at 097E5B94>
```

Fig. 21

Fig. 22